

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-198622

(43) 公開日 平成10年(1998) 7月31日

(51) Int. Cl. <sup>6</sup>	識別記号	F I	
G 0 6 F 13/00	3 5 7	G 0 6 F 13/00	3 5 7 Z
H 0 4 L 12/40		H 0 4 L 11/00	3 2 1

審査請求 未請求 請求項の数11 F D (全 10 頁)

(21) 出願番号 特願平8-359125  
(22) 出願日 平成 8 年(1996) 12月28日

(71) 出願人 000001443  
カシオ計算機株式会社  
東京都渋谷区本町1丁目6番2号  
(72) 発明者 長瀬 公広  
東京都羽村市栄町8丁目2番1号 カシオ  
計算機株式会社羽村技術センター内  
(72) 発明者 稲垣 滋洋  
東京都羽村市栄町3丁目2番1号 カシオ  
計算機株式会社羽村技術センター内  
(74) 代理人 弁理士 阪本 紀康

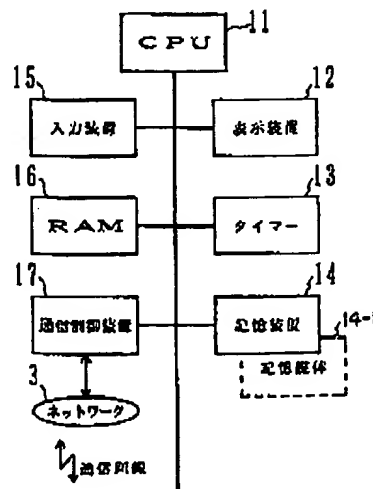
(54) 【発明の名称】 クライアント及びサーバー

(57) 【要約】

【課題】 サーバーコンピュータにログインしているクライアントコンピュータの数が最大ログイン数に達している場合でも、ログインしている必要がないクライアントコンピュータが有る時には、新規のクライアントコンピュータのログインを可能にする。

【解決手段】 ログイン中の各クライアントコンピュータに対してサーバーコンピュータとの最終アクセス時刻をRAM 16に記憶し、新たにクライアントコンピュータからログイン要求が有った場合、あるクライアントコンピュータが上記サーバーコンピュータに対して設定時間以上アクセスが無いことを確認したら、そのクライアントコンピュータをログアウトし、新たなログイン要求を受け付ける。

本発明の実施例における  
サーバーコンピュータ及びクライアントコンピュータの  
システム構成図



(2)

特開平10-198622

2

## 【特許請求の範囲】

【請求項1】 クライアントがサーバーにログインをしてそのクライアントがサーバーに対してアクセスを行い、そのアクセスが終了したらタイマー手段により計測を始め、そのタイマー計測中に上記クライアントが上記サーバーに対して再びアクセスを行ったら上記タイマー手段のリセットを行い、上記クライアントが上記サーバーに対して再びアクセスを行わないまま上記タイマー手段の計測値が第1の設定時間に達したら、上記クライアントをログアウトさせることを特徴とするクライアントにおけるログイン管理方法。

【請求項2】 上記タイマー手段の計測値が上記第1の設定時間に達したら、上記ログアウトと共に上記タイマー手段による計測を始め、その計測中に上記クライアントにおいて入力操作が行われたら上記タイマーの計測を中止し上記クライアントを再びログインさせ、上記クライアントにおいて入力操作が無いままタイマー手段の計測値が第2の設定時間に達したら、上記クライアントを再びログインさせることを特徴とする請求項1に記載のクライアントにおけるログイン管理方法。

【請求項3】 クライアントからサーバーにログインをしてそのクライアントがサーバーに対してアクセスを行い、そのアクセスが終了し、サーバーとのアクセスが必要な登録されたプログラムが動作中になくなら、上記クライアントをログアウトさせることを特徴とするクライアントにおけるログイン管理方法。

【請求項4】 ログアウト状態で有る場合には入力操作の監視を行い、その監視中にサーバーとのアクセスが必要な登録されたプログラムが動作されたら、上記クライアントを再びログインさせることを特徴とするクライアントにおけるログイン管理方法。

【請求項5】 ログインされた各クライアント毎にアイドル状態の監視を行い、ログイン数が最大数に達した状態で新たなクライアントからのログイン要求がある場合、上記アイドル状態が所定の設定時間に達したクライアントの内でアイドル時間が最も長いクライアントをログアウトさせることを特徴とするサーバーにおけるログイン管理方法。

【請求項6】 サーバーにログインを行うための入力を行う入力手段と、  
上記サーバーに接続する通信制御手段と、  
ログイン中に上記サーバーとのアクセスが終了すると起動する第1のタイマー手段と、  
上記入力手段による上記サーバーへのログインとログアウトと、上記第1のタイマー手段が所定の設定時間に達した場合のログアウトを制御する制御手段と、を備えたことを特徴とするクライアント。

【請求項7】 上記第1のタイマー手段が上記第1の設定時間に達した場合に起動する第2のタイマー手段をさらに有し、

上記記憶手段には、上記第2のタイマー手段用の第2の設定時間が記憶され、

上記制御手段は、上記第2のタイマー手段が、上記第2の設定時間に達したら再びログイン処理を行うことを特徴とする請求項6に記載のクライアント。

【請求項8】 複数のクライアントと個別に接続する通信制御手段と、

上記クライアントがログイン中にアクセスが終了すると起動して各クライアント毎にその時間を計測するタイマー手段と、

上記クライアント毎に、上記クライアントとの最終アクセス時刻と上記タイマー手段の第1の設定時間を記憶する記憶手段と、

上記クライアントからの要求による上記クライアントのログインとログアウトと、上記タイマー手段が上記第1の設定時間に達した場合のログアウトを制御し、ログイン可能なクライアント数が満杯である場合のログインしていないクライアントからのログイン要求に対して、上記タイマー手段の計測時間が上記第1の設定時間に達したログイン中のクライアントを強制的にログアウトさせて、新規にログイン要求中のクライアントをログインさせる制御手段と、  
を備えることを特徴とするサーバー。

【請求項9】 コンピュータにおいて用いられたとき、各クライアントがサーバーに対してログインを行ってアクセスした場合に、上記各クライアントの最終アクセスからの時間を各クライアント毎に計測する機能と、  
最終アクセスからの上記計測時間が、予め設定された第1の時間に達したクライアントがあった場合、そのクライアントをログオフさせる機能と、  
を前記コンピュータに行わせるためのプログラムコードが、前記コンピュータが読みとり可能な形式で記憶された記憶媒体。

【請求項10】 各クライアントが、上記第1の設定時間に達してログアウトしたら、そのログアウトからの時間を各クライアント毎に計測する機能と、  
上記ログアウトからの上記計測時間が、設定された第2の時間に達したクライアントがあった場合、そのクライアントを再度ログインさせる機能と、  
を前記コンピュータに行わせるためのプログラムコードが、前記コンピュータが読みとり可能な形式で記憶された請求項9に記載の記憶媒体。

【請求項11】 コンピュータにおいて用いられたとき、  
サーバーへのログイン中に、このサーバーに対するアクセスが終了するとタイマー手段に時間計測を開始させる機能と、  
前記タイマー手段で計測された時間が所定の設定時間に達した場合に前記サーバーからログアウトさせる機能と、

(3)

特開平10-198622

3

4

を前記コンピュータに行わせるためのプログラムコードが、前記コンピュータが読みとり可能な形式で記憶された記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信回線に接続されたクライアントとサーバーに関する。

【0002】

【従来の技術】従来の通信回線に接続された端末装置（端末）とサーバー装置では、一般的に物理的に設置された端末の数よりもサーバー装置と一度に通信接続される端末の数は少なく限られて設定されている。例えば、一つのサーバー装置に通信接続可能な端末が100台であったとしても、同時にそのサーバー装置とログインできるのは40台に限定されるようになっている。これは、一般的には端末の平均したサーバー装置とのログイン時間や1ヶ月の総ログイン時間等から同時に使用される端末の数を仮定して、その数値に有る程度の余裕を持たせて通信回線の容量やサーバー装置側の計算容量あるいはログイン容量を決定しているためである。また、100台の端末に対してそれらの100台の端末がログイン可能にサーバー装置側を対応させようとする、その為のサーバー装置側の設備投資金額や維持費用は40台端末をログイン可能にする場合に比べて遥かに高額になり、時間当たりの各端末の使用率は低下するのでコストパフォーマンスの悪いシステムになってしまうので、一般的には実際に通信回線に接続されている端末数よりもサーバー装置と同時にログイン可能な端末数は低く設定される。

【0003】

【発明が解決しようとする課題】上記のようにサーバー装置側の能力は平均値や集計したデータに基づき決定されているが、実際に端末を使用してサーバー装置にログインする場合には、各端末の使用頻度は各ユーザーの都合により個別で独自に変わり、各端末の使用頻度は管理されているわけではないので、往々にして端末の使用が集中する時間帯が発生する。例えば、朝の山社直後の自分の電子メールの確認、決算日や締め日等の入力の中で、問題発生時のデータ出力等の場合には、端末側のサーバー装置とのログイン希望が、サーバー装置の能力を超えてログイン要求が集中することがあり得る。このような場合には、後からサーバー装置にログインしようと試みた端末の利用者は緊急にサーバー装置にログインしたい場合であってもサーバー装置からログインを拒否されてしまい、ログイン可能になるのを待つしか方法はなかった。

【0004】上記のように端末のサーバー装置へのログインがいつでも可能というわけではないと、偶然あるいは他意なくログイン中に席を外したり、緊急の他の仕事が入ってしまったらしてログアウトしないままに端末が

放置される場合の他にも、例えば、ログインの集中する時間は一度サーバー装置からログアウトすると次にログインできるまでに時間がかかるため、一つの業務は終わっても次の業務のログインのために意図的に端末をログインにしたままに放置しておく場合があり、そのような時にサーバー装置にログインされている端末の台数が、既に予め定められた所定台数以上となっている場合には、後から別の端末で緊急にログインしようとした端末の利用者は、ログインしようとしてもログイン可能となるまで待つしかないという事態が発生している。

【0005】本発明の課題は、そのようなうっかり端末のログアウトを忘れて放置してしまった場合や、意図的に端末をログインしたまま放置している場合に、緊急用のログインが可能ないように放置された端末のログアウトを可能にするものである。

【0006】

【課題を解決するための手段】本発明は、クライアントがサーバー装置にログインをしてそのクライアントとサーバー装置に対してアクセスを行い、そのアクセスが終了したらタイマー手段により計測を始め、そのタイマー計測中に上記クライアントが上記サーバー装置に対して再びアクセスを行ったら上記タイマー手段のリセットを行い、上記クライアントが上記サーバー装置に対して再びアクセスを行わないまま上記タイマー手段の計測値が第1の設定時間に達したら、上記クライアントをログアウトさせることを特徴とする。

【0007】本発明によれば、サーバー装置にログインした端末は、個々にサーバー装置と各端末とのアクセス終了からの経過時間がタイマーにより計測され、次のアクセスが無いまま経過時間が設定された時間に達したらログアウトされるので、端末の利用者がうっかりログオフを忘れてしまった場合や、サーバー装置とのアクセスは行わずに意図的にログオンを続けている使用者がいる場合に、緊急の新規ログオン希望者がログオンできないということがなくなる。

【0008】

【発明の実施の形態】以下に図面を参照しながら本発明の実施例を説明する。図1は本発明の実施例のシステムの全体構成を示す図である。図1のサーバーコンピュータ（サーバー装置）1はネットワーク3により複数のクライアントコンピュータ2と接続されており、データの保管や計算処理、あるいは電子メールの管理等様々な処理を行うものである。クライアントコンピュータ（クライアント）2は、サーバーコンピュータ1に対してはユーザー側の入出力端末として機能するが、それ自体でもスタンドアロンのパーソナルコンピュータやワークステーションとしての機能を持つものである。この図1は一般的なサーバーコンピュータとクライアントコンピュータの関係を示しているが、本発明においてもこのような構成は同様である。

(4)

特開平10-198622

5

6

【0009】図2は、本発明のサーバーコンピュータ1、又は、クライアントコンピュータ2の内部構成を示す図である。CPU11は、クライアントコンピュータ2、又は、サーバーコンピュータ1全体を制御する中央処理装置である。

【0010】入力装置15は、キーボード、マウス等より成り、サーバーコンピュータ1に対するログイン又はログアウトや、電子メール作成のための文字入力やコマンドの選択指示等を行うための装置である。

【0011】表示装置12は、クライアントコンピュータ2の現在の動作状態や入力内容、サーバーコンピュータ1からネットワーク3を介して送られてくる処理結果などのデータ等を表示するディスプレイである。

【0012】RAM16は、上記のコンピュータ1、2の動作状態や入力内容、データ、あるいはアプリケーションプログラム等を一時的に記憶するメモリである。通信制御装置17は、上記ネットワーク3と接続して、このネットワーク3に接続された他のクライアントコンピュータ2やサーバーコンピュータ1と、データや電子メール等の送信・受信を行うものである。

【0013】ネットワーク3は、専用通信回線網によるLAN（ローカル・エリア・ネットワーク）、あるいはWAN（ワイド・エリア・ネットワーク）、又は公衆通信回線網であっても良い。

【0014】タイマー13は、各クライアントコンピュータ2毎にそれぞれのサーバーコンピュータ1との最終アクセスからの時間を計測し、ログアウトした場合は、そのログアウトからの時間を計測するために用いられるものであり、所定時間間隔でCPU11に対して割り込みを行う。

【0015】記憶装置14は、例えばROM、RAM、フラッシュメモリ、HDD（ハードディスクドライブ）記憶装置等からなる記憶媒体14-1を有し、この記憶媒体14-1はCPU11による各種制御に用いられるOS（オペレーティングシステム）と、少なくとも本実施形態のサーバーコンピュータ1またはクライアントコンピュータ2の機能を実現するアプリケーションプログラム等を記憶している。

【0016】また、記憶装置14に設けられる記憶媒体14-1は可搬型のもも含まれる。記憶媒体14-1は少なくとも本実施形態のサーバーコンピュータ1またはクライアントコンピュータ2の機能を実現するアプリケーションプログラムを、記憶装置14内の記憶媒体制御部（不図示）等によって読み出し可能で且つCPU11により実行可能な形式で記憶している。

【0017】また、記憶媒体14-1は、例えば、FD（フロッピーディスク）、MO（光磁気ディスク）、CD-ROM、メモリカード、DVD等により構成してもよく、上記アプリケーションプログラム等を、磁氣的、あるいは光学的、又は電気的に記憶している。

【0018】また、上記アプリケーションプログラムは、例えば、上記通信制御装置17によって、ネットワーク3を介して、サーバーコンピュータ1からダウンロードされたものでよい。この場合、上記記憶装置14の記憶媒体14-1に、上記ダウンロードしたアプリケーションプログラムを記憶して利用するようにしても良い。あるいは、上記通信制御装置17を介して、その接続先のサーバーコンピュータ1等から、それに記憶されている上記アプリケーションプログラムのプログラムコードを、必要に応じてオンラインで受信しながら利用するものであっても良い。

【0019】図3は、サーバーコンピュータ1における、本実施形態における各クライアントコンピュータの管理のための記憶部分と、本実施例のログアウト判定に使われる基準時間の記憶部分の構成を示す。

【0020】本図の記憶部分は例えばRAM16等に設けられる。クライアント管理メモリ20は、各クライアントコンピュータがサーバーコンピュータとの最終アクセスを行った時刻とそれによるアクセスを行っていないアイドル時間が長い順序を記憶するもので、このクライアント管理メモリ20は、後述する図4を用いてさらに詳しく説明する。

【0021】非アクセス基準時間メモリ21は、サーバーコンピュータ1側における、上記の各クライアントコンピュータ2のアイドル時間の限度を示す値を記憶するものであり、後述するタイマー13により測定されるアイドル時間がこのメモリ21に記憶された時間となったら、当該クライアントコンピュータ2をログアウトするためのものである。

【0022】図4は、上記した図3のクライアント管理メモリ20の構成をさらに詳しく示す図である。クライアントNo. 1のクライアントコンピュータ2のメモリデータ31は、前回のサーバーコンピュータ1との最終アクセス時刻である14時30分21秒を記憶し、その時刻がこの図4に表示された5台のクライアントコンピュータ2の中では2番目に現在時刻に近い時間であることから、アイドル時間の順位は4となっている。

【0023】次に、クライアントNo. 4のクライアントコンピュータ2のメモリデータ34は、前回のサーバーコンピュータ1との最終アクセス時刻である3時01分00秒を記憶し、その時刻がこの図4に表示された5台のクライアントコンピュータ2の中では最も現在時刻から遠い時間であることから、アイドル時間の順位は1となっている。

【0024】同様に、クライアントNo. 2、3、5のクライアントコンピュータ2のメモリデータ32、33、35についても、最終アクセス時間とアイドル時間順位が記憶され、アイドル時間が図3の非アクセス基準時間メモリ21に設定されている時間に達する毎にアイドル時間順位の高いクライアントコンピュータ2からロ

(5)

特開平10-198622

7

グアウトされることになる。

【0025】図5は、本実施形態における各クライアントコンピュータ2のログイン及びログアウトの自己管理のために用いられるRAM16又は記憶装置14に設けられる記憶領域の構成を示す。

【0026】設定時間記憶部A41は、本実施例のログアウト判定に使われる基準時間（設定時間A）が設定される記憶領域である。設定時間記憶部B42は、本実施例のログアウト後、再びログインする判定に使われる基準時間（設定時間B）が設定される記憶領域である。

【0027】タイマーA43は、図2のタイマー13からの割り込みによってCPU11によって計測された計時値を記憶するものであり、サーバーコンピュータ1との最終アクセスからの経過時間を記憶しておくための記憶領域である。

【0028】タイマーB44は、上記タイマーAと同様に図2のタイマー13からの割り込みによってCPU11によって計測された計時値を記憶する記憶領域であり、クライアントコンピュータ2がサーバーコンピュータ1からログアウトしてから経過時間を記憶しておくためのものである。

【0029】フラグ45は、クライアントコンピュータ2がログアウトした場合に、そのクライアントコンピュータ2が、利用者からのログアウト入力ではなく自動的にログアウト中の状態になっていることを通常の利用者によるログアウトと区別して示すためのもので、自動ログアウト後にタイマーにより上記設定時間Bに等しい時間まで経過したら該クライアントコンピュータ2をログイン復帰させる場合にはその目印となるものである。

【0030】図6は、クライアントコンピュータ2における本発明の第1の実施例の処理を説明するフローチャートである。なお、このフローチャート及び後述する図7、図8、図9、図10のフローチャートに記述されている各機能を実現するためのプログラムは、CPU11が読み取り可能なプログラムコードの形態で記憶媒体14-1に記憶されている。

【0031】クライアントコンピュータ2が何かの処理を行っている最中に、図2に図示されたタイマー13からの割り込みによって、CPU11により図6に示すネットワーク監視処理が実行される。

【0032】最初にそのクライアントコンピュータ2がサーバーコンピュータ1とログインしているか否かを判別し（ステップS1）、ログインしていない場合には（ステップS1、NO）ログインの復帰処理（ステップS8）へ進み、ログインしている場合には（ステップS1、YES）アイドル中であるかどうかの判別を行う（ステップS2）。

【0033】アイドル中の場合には（ステップS1、YES）、タイマーA43の設定時間の値をカウントアップさせるが（ステップS3）、アイドル中でない場合

8

は、クライアントコンピュータ2は起動されていないということなので、タイマーA43をリセットする（ステップS7）。

【0034】タイマーA43の設定時間をカウントアップすると（ステップS3）、このタイマーA43の設定時間が設定時間Aを超えたかどうかを判別し（ステップS4）、設定時間を超えていなければ（ステップS4、NO）割り込み前の元の処理に復帰するが、設定時間Aを超えていると判定した場合には（ステップS4、YES）ログアウト処理を行い（ステップS5）、次に自動的にログアウト処理が行われたことを示すためにフラグ45をONする（ステップS6）。

【0035】そのログアウト処理後、タイマーA42の設定時間をリセットして（ステップS7）、次に割り込み前の元の処理に復帰する。このようにして、サーバーコンピュータ1との最終アクセス後に設定時間記憶部A41に設定された設定時間Aが経過したクライアントコンピュータ2は、自らの判定によりログアウトする。

【0036】図7は、クライアントコンピュータ2における、図6のログイン復帰処理（ステップS9）をさらに詳しく説明するフローチャートである。図6のログイン中であるかの確認（ステップS1）でログイン中でない場合には、CPU11はこのログイン復帰処理（ステップS8）を行う。このログイン復帰処理では、まず、図6のステップS5による自動ログアウト状態であるのかそれとも他の理由によるログアウト状態であるのかを知るためにフラグ45がONされているか否かを判別する（ステップS11）。

【0037】フラグ45がONに設定されていなければ（ステップS11、NO）、上記ステップS5による自動ログアウト状態ではないのでタイマーBの設定時間をリセットして（ステップS17）処理を終了するが、フラグ45がONに設定されている場合には上記ステップS5による自動ログアウト状態であるので、タイマーB43の設定時間をカウントアップする（ステップS12）。

【0038】タイマーB43の設定時間をカウントアップした（ステップS12）後、タイマーB43の設定時間が、設定時間記憶部B42に設定されている設定時間Bを経過したかどうかを判別し（ステップS13）、設定時間Bを経過していない場合には（ステップS13、NO）タイマーB43の設定時間をリセットして（ステップS17）処理を終了するが、設定時間B以上を経過していた場合にはログイン可能か否かの判定を行う（ステップS14）。

【0039】このステップS14では、クライアントコンピュータ2側ではログインを行おうとするが、サーバーコンピュータ1側ではログインを受け付けられない場合もあるので、ログイン可能か否かの確認が行われ、サーバーコンピュータ1側の拒絶等でログインできなかった

10

20

30

40

50

(6)

特開平10-198622

9

10

た場合(ステップS14、NO)には、フラグ45をそのままにしてタイマーH43の設定時間Hをリセット

(ステップS17)して処理を終了するが、ログインがOKの場合(ステップS14、YES)には、ログイン処理を行い(ステップS15)、フラグをOFFし(ステップS16)、タイマーの設定時間Bをリセットして(ステップS17)処理を終了する。

【0040】図8は、クライアントコンピュータ2における本発明の第1実施例でのログアウト中の、クライアントコンピュータ2の人力操作の監視処理を示すフローチャートである。

【0041】図6のステップS5でクライアントコンピュータ2により自動的にログアウト処理が行われた場合でも、その後そのクライアントコンピュータ2で人力操作が行われた場合には自動的にログイン処理が行われるように、この入力操作監視処理が行われる。

【0042】この入力操作監視処理では、まず、入力操作が行われたかどうかを判別し(ステップS21)、人力操作が無い場合には(ステップS21、NO)元の表示処理へ復帰する(ステップS26)が、入力操作が行った場合には(ステップS21、YES)、フラグ45がONに設定されているかどうかを判別する(ステップS22)。

【0043】そして、フラグ45がONに設定されていない場合には(ステップS22、NO)、元の表示処理に復帰する(ステップS26)であるが、フラグ45がONの場合は(ステップS22、YES)、ログイン可能かの判定が行われる(ステップS23)。

【0044】このステップS23においても、上記図7のステップS14の場合と同様に、サーバーコンピュータ1側の都合でログインが拒絶される場合があるので、ログインOKかの確認が行われるが、ログインができない場合(ステップS23、NO)には、元の表示処理に復帰(ステップS26)するが、ログインできた場合(ステップS23、YES)には、ログイン処理が行われ(ステップS24)、フラグ45がOFFされて(ステップS25)、元の表示処理に復帰(ステップS26)する。

【0045】図9は、クライアントコンピュータ2における、本発明の第2の実施例を示すフローチャートである。図6の場合と同様に図2に示すタイマー13による割り込み処理で本発明の第2の実施例のネットワーク監視処理へ入る。

【0046】この第2の実施例では、まず、クライアントコンピュータ2内で、予め登録されているネットワーク3に対応した(サーバーコンピュータ1にアクセスする)アプリケーション(登録アプリケーション)が起動されているかどうかを判別する(ステップS31)。

【0047】上記の登録アプリケーションが起動中の場合は(ステップS31、YES)、次にログイン中であ

るかどうかを判別し(ステップS32)、ログイン中の場合は(ステップS32、YES)、割り込み前の元の処理に戻るが、ログインしていなかった場合には(ステップS32、NO)、ログイン処理を行ってから(ステップS33)元の処理に戻る。

【0048】一方、上記の登録アプリケーションが起動中でなかった場合には(ステップS31、NO)、やはり、ログイン中であるかどうかを判別し(ステップS34)、ログインしていなかった場合には(ステップS34、NO)、割り込み前の元の処理に戻るが、ログイン中であった場合には(ステップS34、YES)、ログアウト処理を行ってから(ステップS35)、元の処理に戻る。

【0049】このようにして、サーバーコンピュータ1とログインしていることが必要でないアプリケーションが起動しているクライアントコンピュータ2は、自らの判定によりログアウトする。

【0050】図10は、本発明のサーバーコンピュータ1における本発明に係わる実施例の処理を説明するフローチャートである。サーバーコンピュータ1は、まず、クライアントコンピュータ2からログインの要求があるかどうかを判別する(ステップS41)。

【0051】ログインの要求がない場合には(ステップS41、NO)、特に本実施例の処理を行う必要はないので再び、ステップS41に戻るが、ログイン要求があった場合には(ステップS41、YES)、そのサーバーコンピュータ1において、現在ログインしているクライアントコンピュータ2の数が最大ログイン数に達しているかを判別する(ステップS42)。

【0052】そして、最大ログイン数に達していない場合には(ステップS42、NO)強制ログアウト処理は必要なくログインを受け付ける(ステップS47)。一方、ログイン数が最大数に達していた場合は(ステップS42、NO)、次に、所定時間以上アクセスしていないクライアントコンピュータ2が存在するかどうかをクライアント管理メモリ20を参照して確認する(ステップS43)。

【0053】ここで、該当するクライアントコンピュータ2が無い場合は(ステップS44、NO)、新規にログインを希望しているクライアントコンピュータ2に対してログインを拒否する(ステップS46)が、該当するクライアントコンピュータ2が有った場合には(ステップS44、YES)、その該当するクライアントコンピュータ2をログアウトさせ(ステップS45)、新たにログインを要求してきたクライアントコンピュータ2をログインさせる(ステップS47)。

【0054】このようにして、サーバーコンピュータ1側で、ログインしているクライアントコンピュータ2が最大ログイン数に達している場合に、新たなクライアントコンピュータ2からログイン要求が来た場合、前回

(7)

特開平10-198622

11

のアクセスから所定時間以上が経過しているクライアントコンピュータ2が存在する場合にはそのクライアントコンピュータ2を強制的にログアウトさせ、新たなログイン要求を受け入れることができるようになる。

【0055】尚、上記実施例では本発明をサーバーと複数のクライアントで構成されるクライアントサーバーシステムに適用した例を示したが、本発明はこれに限定されるものではなく、メインフレームと複数の端末で構成されるシステムにも適用可能なものである。

【0056】

【発明の効果】本発明によれば、従来はサーバーコンピュータに対してログインしているクライアントコンピュータ（端末）の台数が、システムで予め設定されている最大数に達していた場合には、新規にログインを希望するクライアントコンピュータがあっても、そのログイン要求を拒否せざるを得なかったが、本発明によれば、うっかりログアウトを忘れた人や使用していないにも関わらずログインを継続している人をログアウトにできるので、ログインを希望するユーザーを待たせる場合を減らすことができ、ネットワーク全体を効率的に運用できるようになる。

【図面の簡単な説明】

【図1】本発明の実施例の全体構成を示す図である。

【図2】本発明の実施例におけるサーバーコンピュータ及びクライアントコンピュータのシステム構成図である。

【図3】本実施例のサーバーコンピュータの記憶装置の構成を説明する図である。

【図4】図3のクライアント管理メモリの構成を説明する図である。

【図5】本発明の第1の実施例のクライアントコンピュータの記憶装置の構成を説明する図である。

【図6】本発明の第1実施例のクライアントコンピュ

12

タにおけるネットワーク監視処理を説明するフローチャートである。

【図7】図6のフローチャートにおけるログイン復帰処理の動作を説明するフローチャートである。

【図8】本発明の第1の実施例のクライアントコンピュータにおける入力操作監視処理を説明するフローチャートである。

【図9】本発明の第2の実施例のクライアントコンピュータにおけるネットワーク監視処理を説明するフローチャートである。

【図10】本発明の実施例のサーバーコンピュータの動作を説明するフローチャートである。

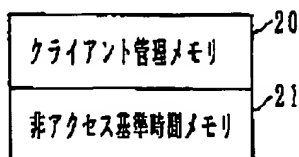
【符号の説明】

- 1 サーバーコンピュータ
- 2 クライアントコンピュータ
- 3 ネットワーク
- 11 CPU
- 12 表示装置
- 13 タイマー
- 14 記憶装置
- 14-1 記憶媒体
- 15 入力装置
- 16 RAM
- 17 通信制御装置
- 20 クライアント管理メモリ
- 21 非アクセス基準時間メモリ
- 32、33、34、35 クライアントコンピュータの最終アクセス時刻とアイドル時間順位
- 41 設定時間記憶部A
- 42 設定時間記憶部B
- 43 タイマーA
- 44 タイマーB
- 45 フラグ

【図3】

本実施例のサーバーコンピュータの  
記憶装置の構成を説明する図

16

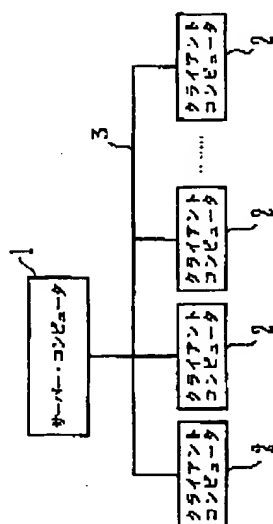


(8)

特開平10-198622

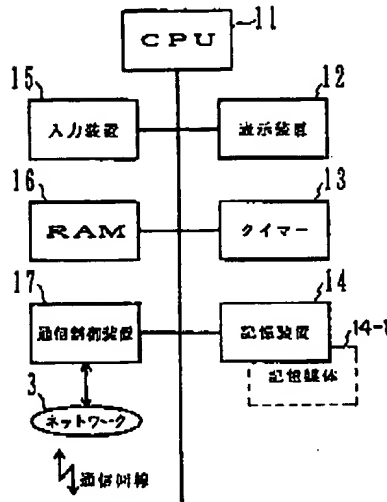
【図1】

本発明の実施例の全体構成を示す図



【図2】

本発明の実施例における  
サーバコンピュータ及びクライアントコンピュータの  
システム構成図



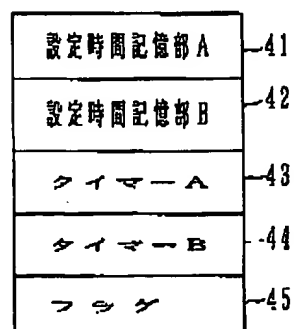
【図4】

図3のクライアント管理メモリの構成を説明する図

クライアントNo.	最終アクセス時刻	アイドル時間順位
1	14:30:21	4
2	14:00:00	3
3	15:35:10	5
4	03:01:00	1
5	05:08:30	2
...	...	...

【図5】

本発明の第1の実施例のクライアントコンピュータの  
記憶装置の構成を説明する図



20

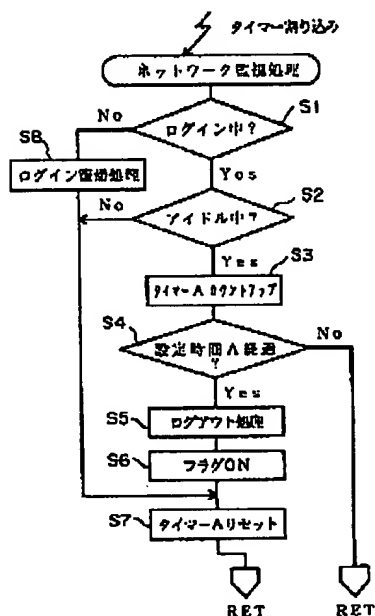


(9)

特開平10-198622

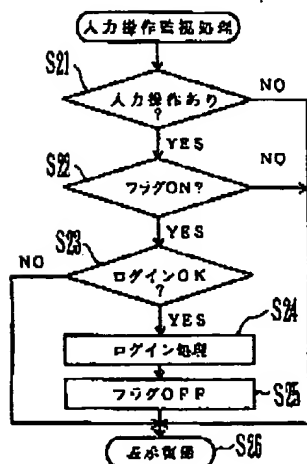
【図6】

本発明の第1実施例のクライアントコンピュータ  
におけるネットワーク監視処理を説明するフローチャート



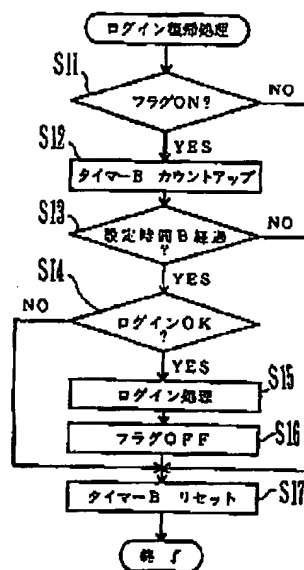
【図8】

本発明の第1実施例のクライアントコンピュータ  
における入力操作監視処理を説明するフローチャート



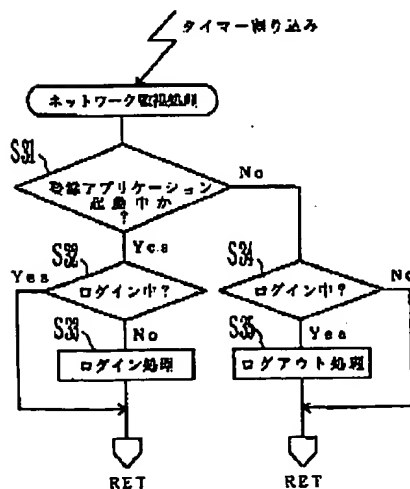
【図7】

図6のフローチャートにおける  
ログイン復帰処理の動作を説明するフローチャート



【図9】

本発明の第2実施例のクライアントコンピュータ  
におけるネットワーク監視処理を説明するフローチャート

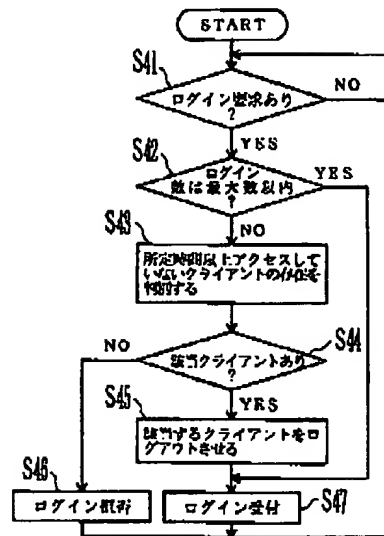


(10)

特開平10-198622

## 【図10】

本発明の実施例のサーバコンピュータの  
動作を説明するフローチャート



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKewed/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**